

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-111835
(43)Date of publication of application : 28.04.1998

(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 08-264606

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 04.10.1996

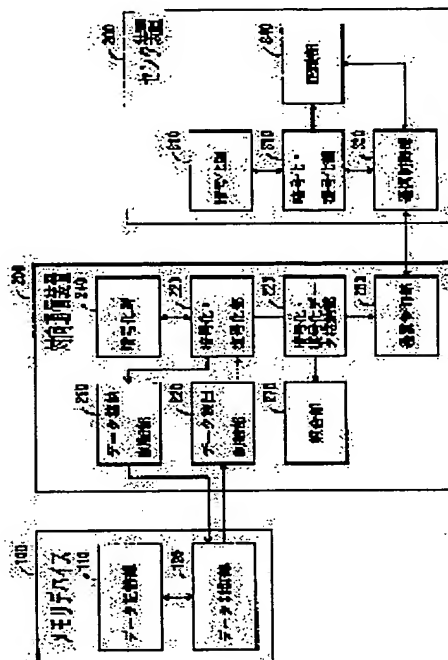
(72)Inventor : SAKIDA KAZUTAKA
SHIMADA IKUKO
ISHIGURO GINYA

(54) METHOD AND SYSTEM FOR IN-USE DEVICE ID TRANSMISSION

(57)Abstract:

PROBLEM TO BE SOLVED: To correctly transfer and manage an ID without receiving an illegal information report, etc., by applying a ciphering rule having a parameter to an opposite communication device and ciphering data, and writing the ciphered data and parameter in a memory device.

SOLUTION: The opposite communication device 200 ciphers data including the memory device ID of the memory device 100 as a written object according to the ciphering rule 240 having the parameter and transfers the data to the memory device 100 from a data storage control part 210. The memory device 100 stores the data in a data storage part 110. Then when the opposite communication device 200 writes to the memory device 100 thereafter, a data read control part 220 transfers a readout command and the memory device 100 extracts the ciphered data from the parameter and transfers them. The opposite communication device 200 deciphers the data by using the ciphering rule 240 and specifies the ID of the memory device 100.



LEGAL STATUS

[Date of request for examination] 11.01.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

BEST AVAILABLE COPY

②

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 0 - 1 1 1 8 3 5

(43) 公開日 平成 1 0 年 (1 9 9 8) 4 月 2 8 日

(51) Int. Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G06F 12/14	320		G06F 12/14	320 B
12/00	510		12/00	510 A

審査請求 未請求 請求項の数 1 3 O L (全 2 4 頁)

(21) 出願番号 特願平 8 - 2 6 4 6 0 6
(22) 出願日 平成 8 年 (1 9 9 6) 1 0 月 4 日

(71) 出願人 0 0 0 0 0 4 2 2 6
日本電信電話株式会社
東京都新宿区西新宿三丁目 1 9 番 2 号
(72) 発明者 崎田 一貴
東京都新宿区西新宿三丁目 1 9 番 2 号 日
本電信電話株式会社内
(72) 発明者 嶋田 郁子
東京都新宿区西新宿三丁目 1 9 番 2 号 日
本電信電話株式会社内
(72) 発明者 石黒 銀矢
東京都新宿区西新宿三丁目 1 9 番 2 号 日
本電信電話株式会社内
(74) 代理人 弁理士 伊東 忠彦

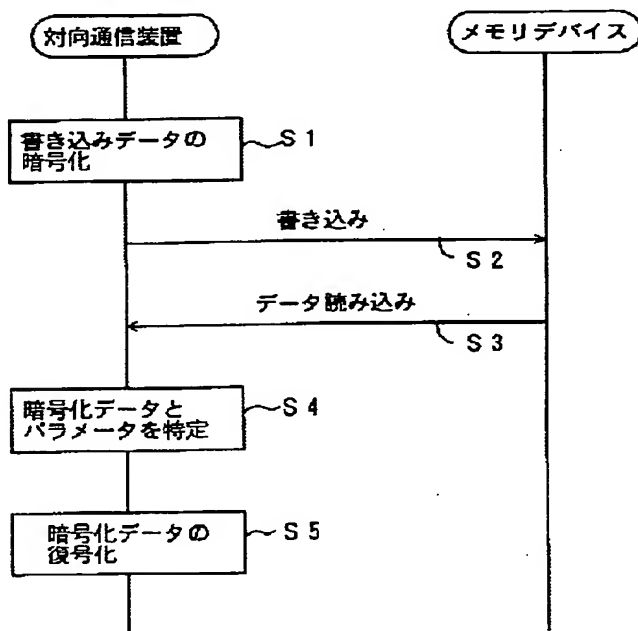
(54) 【発明の名称】 使用装置 I D 伝達方法及びシステム

(57) 【要約】

【課題】 各メモリデバイス毎にその I D 情報と何らかの運用履歴情報を追跡管理する必要がある時に、 I D 管理等を不正情報通知等を受けることなく、正しくやり取りし、管理することが可能な使用装置 I D 伝達方法及びシステムを提供する。

【解決手段】 本発明は、メモリデバイス I D を含むデータをパラメータを有する暗号化則を適用してデータを暗号化し、暗号化されたデータとパラメータをメモリデバイスに書き込み、メモリデバイスからデータを読み込んで、暗号化されたデータとパラメータを特定し、パラメータを有する暗号化則を適用して読み込んだデータを復号化する。

本発明の原理を説明するための図



【特許請求の範囲】

・【請求項 1】 複数のメモリデバイスと複数の対向通信装置及びセンタ装置及び通信回線設備から構成されるシステムにおける、使用デバイス ID や使用対向通信装置 ID を追跡管理するために該 ID を伝達する使用装置 ID 伝達方法において、

・前記メモリデバイスに該メモリデバイス ID を含むデータを書き込む際に、前記対向通信装置においてパラメータを有する暗号化則適用してデータを暗号化し、暗号化されたデータと前記パラメータを前記メモリデバイスに書き込み、

前記メモリデバイスからデータを読み込む際に、該メモリデバイスからデータを読み込んで、暗号化されたデータと前記パラメータを特定し、

前記パラメータを有する暗号化則を適用して読み込んだ前記データを復号化することを特徴とする使用装置 ID 伝達方法。

【請求項 2】 前記メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、前記メモリデバイス ID を含むデータをパラメータを含む暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、

それ以降にデータを書き込む第 2 の対向通信装置が、前記メモリデバイスからデータを読み込んで、前記パラメータと前記暗号化されたデータとを抽出し、

前記暗号化されたデータを前記パラメータを有する暗号化則で復号し、メモリデバイス ID を特定した後、該メモリデバイス ID を含むデータを、パラメータを有する暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、

前記センタ装置が、前記メモリデバイスに書き込まれていた前記データをそのままの形式か、もしくは対向通信装置が変形した形式で、対向通信装置から通信回線を介して受け取り、受信データから暗号化データと前記暗号化則のパラメータを抽出し、該暗号化データをパラメータを有する暗号化則で復号して、前記メモリデバイス ID を特定する請求項 1 記載の使用装置 ID 伝達方法。

【請求項 3】 前記メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、

書き込み対象のメモリデバイスのメモリデバイス ID と対向通信装置 ID を含むデータを、パラメータを有する暗号化側で暗号化して、該パラメータと暗号化データを該メモリデバイスに書き込み、

それ以降にデータを書き込む第 2 の対向通信装置が、

前記メモリデバイスからデータを読み込んで、該パラメータと前記暗号化データをパラメータを有する暗号化側で復号して、該メモリデバイス ID と前記第 1 の対向通信装置の使用対向通信装置 ID を特定した後、該メモリデバイス ID と該第 2 の対向通信装置の対向通信装置 ID を含むデータを、パラメータを有する暗号化側で暗号

化し、該パラメータと暗号化データを該メモリデバイスに書き込み、

センタ装置が、

前記メモリデバイスに書き込まれていた前記データを、そのままの形式か、もしくは、前記対向通信装置が変形した形式で対向通信装置から通信回線を介して受け取り、受信データから暗号化データと暗号化側のパラメータを抽出し、該暗号化データを該パラメータを有する暗号化側で復号して、該メモリデバイス ID と該対向通信装置 ID を特定する請求項 2 記載の使用装置 ID 伝達方法。

【請求項 4】 前記対向通信装置間で暗号化の第 2 のパラメータ、もしくは第 2 の暗号化則を共有し、

前記メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、

該メモリデバイス ID を前記第 2 のパラメータもしくは、前記第 2 の暗号化則で暗号化し、

暗号化された暗号化情報を含むデータを更に、第 1 のパラメータ若しくは、第 1 の暗号化則で暗号化して前記メモリデバイス内に書き込み、

それ以降にデータを書き込む第 2 の対向通信装置が、

前記メモリデバイスからデータを読み込んで、暗号化データを抽出し、該暗号化データを復号して、取得した該メモリデバイス ID と該メモリデバイス ID を前記第 2 のパラメータもしくは、前記第 2 の暗号化則で暗号化した情報を含むデータを特定した後、該特定されたデータを更に、前記第 2 のパラメータもしくは前記第 2 の暗号化則で復号して該メモリデバイス ID を特定し、2 種類得られた該メモリデバイス ID を照合する請求項 2 記載の使用装置 ID の伝達方法。

【請求項 5】 前記メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、

該メモリデバイスが記憶する金額情報を含むカウンタ情報を有するデータと暗号化情報を該メモリデバイス内に書き込み、

それ以降にデータを書き込む第 2 の対向通信装置が、

前記メモリデバイスからデータを読み込んで、前記金額情報を含むカウンタ情報と暗号化データを抽出し、さらに、該暗号化データを復号して、該金額情報を含むカウンタ情報を特定し、2 種類得られた該金額情報を含むカウンタ情報を照合する請求項 2 記載の使用装置 ID 伝達方法。

【請求項 6】 複数のメモリデバイスと複数の対向通信装置、センタ装置及び通信回線設備を有するシステムにおける、使用デバイス ID や使用対向通信装置 ID を追跡管理するために、該使用デバイス ID や該使用対向通信装置 ID を伝達する使用装置 ID 伝達システムであって、

前記メモリデバイスは、

前記対向通信装置の書き込み動作によりデータを記憶す

るデータ記憶手段を有し、

前記対向通信装置は、

書き込み対象のメモリデバイス I D を含むデータを暗号化したデータと、該暗号化のためのパラメータを書き込みデータとして前記メモリデバイスに書き込む書き込み手段と、

前記メモリデバイスから前記メモリデバイス I D を含むデータを暗号化したデータと該暗号化のパラメータを読み込みデータとして読み込むデータ読み込み手段と、

前記センタ装置と情報交信するセンタ交信手段と、

パラメータに応じて暗号化側を変化させて、暗号化、復号化すべき前記メモリデバイス I D を含むデータを暗号化、復号化する第 1 の暗号化・復号化手段と、

前記センタ装置は、

前記対向通信装置と情報交信する対向通信装置交信手段と、

前記対向通信装置交信手段と交信する交信情報から前記メモリデバイス I D を含むデータを暗号化したデータとその暗号化パラメータを読み込む読み込み手段と、

前記パラメータに応じて、暗号化側を変化させて前記メモリデバイス I D を含むデータを暗号化・復号化する第 2 の暗号化・復号化手段とを有することを特徴とする使用装置 I D 伝達システム。

【請求項 7】 前記対向通信装置の前記書き込み手段は、

前記メモリデバイスに書き込むデータとして、当該メモリデバイスのメモリデバイス I D と自対向通信装置 I D を含むデータを暗号化したデータと暗号化に用いる暗号化パラメータを設定する書き込みデータ設定手段を有し、

前記データ読み込み手段は、

前記メモリデバイスから読み込むデータとして当該メモリデバイスのメモリデバイス I D と自対向通信装置 I D を含むデータを暗号化したデータと該暗号化に用いられた暗号化パラメータを設定する読み出しデータ設定手段を有し、

前記センタ装置の前記読み込み手段は、

前記対向通信装置と交信した情報から前記メモリデバイス I D と対向通信装置 I D を含むデータを暗号化した暗号化データと、暗号化の際に用いられた暗号化パラメータを読み込む手段を有し、

前記第 1 の暗号化・復号化手段及び前記第 2 の暗号化・復号化手段は、

前記メモリデバイス I D と前記対向通信装置 I D を含むデータを暗号化・復号化する手段を有する請求項 6 記載の使用装置 I D 伝達システム。

【請求項 8】 前記対向通信装置は、

前記対向通信装置間で、暗号化の第 2 のパラメータもしくは、第 2 の暗号化則を共有する第 2 の暗号化則共有手段と、

前記第 2 の暗号化則共有手段において、共有されている前記第 2 のパラメータもしくは、前記第 2 の暗号化則で暗号化、復号化する第 3 の暗号化・復号化手段と、

前記メモリデバイス I D を前記第 3 の暗号化・復号化手段で暗号化したデータを含むデータを、更に、前記第 1 の暗号化・復号化手段で暗号化して、前記メモリデバイスに格納する暗号化データ格納制御手段と、

前記暗号化格納制御手段により前記メモリデバイスに格納された暗号化データを読み取る暗号化データ読み取り手段と、

前記暗号化データ読み取り手段により取得した前記暗号化データから、2 種類以上の前記メモリデバイス I D を照合する照合手段とを有する請求項 6 記載の使用装置 I D 伝達システム。

【請求項 9】 前記照合手段は、

前記暗号化データ読み取り手段により取得した暗号化データに、前記第 1 の暗号化・復号化手段を適用して特定した前記メモリデバイス I D と、同時に特定される該メモリデバイス I D が前記第 3 の暗号化・復号化手段で暗号化されている部分のデータについて更に、該第 3 の暗号化・復号化手段を適用して特定した前記メモリデバイス I D とを照合する手段を含む請求項 8 記載の使用装置 I D 伝達システム。

【請求項 10】 前記照合手段において、前記メモリデバイス I D が照合できた場合には、前記暗号化データ及び該メモリデバイス I D を暗号化したデータと暗号化パラメータを該メモリデバイス I D に対応する前記メモリデバイスに格納する第 1 の再格納手段を含む請求項 9 記載の使用装置 I D 伝達システム。

【請求項 11】 前記対向通信装置は、

金額情報を含むカウンタ情報を有するデータと該データの暗号化情報を前記メモリデバイスに格納する暗号化情報格納制御手段と、

前記暗号化情報格納制御手段により前記メモリデバイスに格納された前記カウンタ情報及び前記暗号化情報を読み取る暗号化情報読み取り手段と、

前記暗号化情報読み取り手段により取得した 2 種類以上の前記カウンタ情報を照合するカウンタ情報照合手段とを含む請求項 6 記載の使用装置 I D 伝達システム。

【請求項 12】 前記カウンタ情報照合手段は、

前記暗号化情報読み取り手段により取得したカウンタ情報と、前記暗号化情報を復号して特定されたカウンタ情報とを照合する手段を含む請求項 11 記載の使用装置 I D 伝達システム。

【請求項 13】 前記カウンタ情報照合手段において、

前記カウンタ情報が照合できた場合には、該カウンタ情報、メモリデバイス I D と該カウンタ情報を暗号化したデータ、及び暗号化パラメータをメモリデバイス I D に対応するメモリデバイスに格納する第 2 の再格納手段を含む請求項 12 記載の使用装置 I D 伝達システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】本発明は、使用装置 I D 伝達方法及びシステムに係り、特に、メモリデバイスと対向通信装置、及びセンタ装置からなるシステムにおいて、使用したメモリデバイス I D もしくは、使用したメモリデバイス I D を対向通信装置及びセンタ装置が管理し、その I D 管理情報から偽造メモリデバイスの使用やメモリデバイスに成り済ます行為を検知するための使用装置 I D 伝達方法及びシステムに関する。

【 0 0 0 2 】

【従来の技術】複数のメモリデバイスを用いて運用するシステムの中には、各メモリデバイス毎にその I D と何らかの運用履歴情報を追跡管理する必要があるものが存在する。これらのシステムでは、各メモリデバイスから当該メモリデバイスの I D と付帯情報を対向通信装置あるいは、センタ装置に通知している。このとき、当該メモリデバイスの I D が外部から容易に覗くことが可能で、改ざんされたり、当該 I D 相当に成り済まされたりすると、管理システムの機能を果たせない恐れがある。このため、通知される I D の正当性が保証されることが重要である。この点を考慮して、メモリデバイスの I D を暗号化して通知したり、I D にデジタル署名を添付して通知したり、あるいは、それらを併用したりする方法が採られている。

【 0 0 0 3 】

【発明が解決しようとする課題】しかしながら、上記のメモリデバイスで暗号化を行う場合は、当該デバイスに相応の演算能力やデータ記憶量等の計算リソースが必要になり、対向通信装置のみで暗号化を行う場合でも、当該デバイスに相応のデータ記憶量が必要になる。I D にデジタル署名を添付する場合は、更に大量のデータ記憶量が必要になる。コスト要求条件からメモリデバイスにこれらのリソースを装備し得ないシステムでは、従来、デバイスの I D を直接やり取りするケースが多い。

【 0 0 0 4 】しかし、I D を直接やり取りする方法では、I D が外部から容易に覗くことができるため、I D 管理システムは不正情報通知等を受け易い。また、システム構築や運用に際し、上記の危険性は無視できないので、上記の危険性はシステム構築や運用の制限条件となる。

【 0 0 0 5 】一方、メモリデバイスの I D を暗号化してやり取りする方法を採れば、上記の不正情報通知等の可能性が低くなるものの、デバイスの I D の暗号化を行い、暗号化された I D をやり取りする方法を採った場合でも簡易な暗号化規則を採用したり、全システム共通の鍵を用いて暗号化する場合が殆どであるため、複数の情報をモニタして暗号則を推定し、然る後に、不正情報通知等を受ける可能性がある。また、暗号化規則が簡易な場合には、暗号化規則を推定され易い。また、暗号化規

則を標準レベルまで複雑にしても、全システム共通の鍵を用いてしまうと、大量の情報をモニタされた場合に、暗号則を推定される恐れがある。

【 0 0 0 6 】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、メモリデバイスとその対向通信装置及びセンタ装置とからなるシステムにおいて、各メモリデバイス毎にその I D 情報と何らかの運用履歴情報を追跡管理する必要がある時に、I D 管理等を不正情報通知等を受けることなく、正しくやり取りし、管理することが可能な使用装置 I D 伝達方法及びシステムを提供することを目的とする。

【 0 0 0 7 】

【課題を解決するための手段】図 1 は、本発明の原理を説明するための図である。第 1 の発明は、複数のメモリデバイスと複数の対向通信装置及びセンタ装置及び通信回線設備から構成されるシステムにおける、使用デバイス I D や使用対向通信装置 I D を追跡管理するために該 I D を伝達する使用装置 I D 伝達方法において、メモリデバイスにメモリデバイス I D を含むデータを書き込む際に、対向通信装置において、パラメータを有する暗号化則を適用してデータを暗号化し（ステップ 1）、暗号化されたデータとパラメータをメモリデバイスに書き込み（ステップ 2）、メモリデバイスからデータを読み込んで（ステップ 3）、暗号化されたデータとパラメータを特定し（ステップ 4）、パラメータを有する暗号化則を適用して読み込んだデータを復号化する（ステップ 5）。

【 0 0 0 8 】第 2 の発明は、メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、メモリデバイス I D を含むデータを、パラメータを含む暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、それ以降にデータを書き込む第 2 の対向通信装置が、メモリデバイスからデータを読み込んで、パラメータと暗号化されたデータとを抽出し、暗号化されたデータをパラメータを有する暗号化則で復号し、メモリデバイス I D を特定した後、該メモリデバイス I D を含むデータを、パラメータを有する暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、センタ装置が、メモリデバイスに書き込まれていたデータをそのままの形式か、もしくは対向通信装置が変形した形式で、対向通信装置から通信回線を介して受け取り、受信データから暗号化データと暗号化則のパラメータを抽出し、該暗号化データをパラメータを有する暗号化則で復号して、メモリデバイス I D を特定する。

【 0 0 0 9 】第 3 の発明は、メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、書き込み対象のメモリデバイスのメモリデバイス I D と対向通信装置 I D を含むデータを、パラメータを有する暗号化側で暗号化して、該パラメータと暗号化データを該メモリデバイ

スに書き込み、それ以降にデータを書き込む第 2 の対向通信装置が、メモリデバイスからデータを読み込んで、該パラメータと暗号化データをパラメータを有する暗号化側で復号して、該メモリデバイス ID と第 1 の対向通信装置の使用対向通信装置 ID を特定した後、該メモリデバイス ID と該第 2 の対向通信装置の対向通信装置 ID を含むデータを、パラメータを有する暗号化側で暗号化し、該パラメータと暗号化データを該メモリデバイスに書き込み、センタ装置が、メモリデバイスに書き込まれていたデータを、そのままの形式か、もしくは、対向通信装置が変形した形式で対向通信装置から通信回線を介して受け取り、受信データから暗号化データと暗号化側のパラメータを抽出し、該暗号化データを該パラメータを有する暗号化側で復号して、該メモリデバイス ID と該対向通信装置 ID を特定する。

【 0 0 1 0 】第 4 の発明は、対向通信装置間で暗号化の第 2 のパラメータ、もしくは第 2 の暗号化則を共有し、メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、該メモリデバイス ID を第 2 のパラメータもしくは、第 2 の暗号化則で暗号化し、暗号化された暗号化情報を含むデータを更に、第 1 のパラメータ若しくは、第 1 の暗号化則で暗号化してメモリデバイス内に書き込み、それ以降にデータを書き込む第 2 の対向通信装置が、メモリデバイスからデータを読み込んで、暗号化データを抽出し、該暗号化データを復号して、取得した該メモリデバイス ID と該メモリデバイス ID を第 2 のパラメータもしくは、第 2 の暗号化則で暗号化した情報を含むデータを特定した後、該特定データを更に、第 2 のパラメータもしくは第 2 の暗号化則で復号して該メモリデバイス ID を特定し、2 種類得られた該メモリデバイス ID を照合する。

【 0 0 1 1 】第 5 の発明は、メモリデバイスに最初にデータを書き込む第 1 の対向通信装置が、該メモリデバイスが記憶する金額情報を含むカウンタ情報を有するデータと暗号化情報を該メモリデバイス内に書き込み、それ以降にデータを書き込む第 2 の対向通信装置が、メモリデバイスからデータを読み込んで、金額情報を含むカウンタ情報と暗号化データを抽出し、さらに、該暗号化データを復号して、該金額情報を含むカウンタ情報を特定し、2 種類得られた該金額情報を含むカウンタ情報を照合する。

【 0 0 1 2 】図 2 は、本発明の原理構成図である。第 6 の発明は、複数のメモリデバイス 1 0 0 と複数の対向通信装置 2 0 0、センタ装置 3 0 0 及び通信回線設備 4 0 0 を有するシステムにおける、使用デバイス ID や使用対向通信装置 ID を追跡管理するために、該使用デバイス ID や該使用対向通信装置 ID を伝達する使用装置 ID 伝達システムであって、メモリデバイス 1 0 0 は、対向通信装置 2 0 0 の書き込み動作によりデータを記憶するデータ記憶手段 1 1 0 を有し、対向通信装置 2 0 0

は、書き込み対象のメモリデバイス ID を含むデータを暗号化したデータと、該暗号化のためのパラメータを書き込みデータとしてメモリデバイスに書き込む書き込み手段 2 1 0 と、メモリデバイス 1 0 0 からメモリデバイス ID を含むデータを暗号化したデータと該暗号化のパラメータを読み込みデータとして読み込むデータ読み込み手段 2 2 0 と、センタ装置 3 0 0 と情報交換するセンタ装置 2 5 0 と、パラメータに応じて暗号化側を変化させて、暗号化、復号化すべきメモリデバイス ID を含むデータを暗号化、復号化する第 1 の暗号化・復号化手段 2 3 0 と、センタ装置 3 0 0 は、対向通信装置と情報交換する対向通信装置 3 3 0 と、対向通信装置 3 3 0 と交換する交換情報からメモリデバイス ID を含むデータを暗号化したデータとその暗号化パラメータを読み込む読み込み手段 3 4 0 と、パラメータに応じて、暗号化側を変化させてメモリデバイス ID を含むデータを暗号化・復号化する第 2 の暗号化・復号化手段 3 1 0 とを有する。

【 0 0 1 3 】第 7 の発明において、対向通信装置 2 0 0 の書き込み手段 2 1 0 は、メモリデバイス 1 0 0 に書き込むデータとして、当該メモリデバイス 1 0 0 のメモリデバイス ID と自対向通信装置 ID を含むデータを暗号化したデータと暗号化に用いる暗号化パラメータを設定する書き込みデータ設定手段を有し、データ読み込み手段 2 2 0 は、メモリデバイス 1 0 0 から読み込むデータとして当該メモリデバイス 1 0 0 のメモリデバイス ID と自対向通信装置 ID を含むデータを暗号化したデータと該暗号化に用いられた暗号化パラメータを設定する読み出しデータ設定手段を有し、センタ装置 3 0 0 の読み込み手段 3 4 0 は、対向通信装置と交換した情報から、メモリデバイス ID と対向通信装置 ID を含むデータを暗号化した暗号化データと、暗号化の際に用いられた暗号化パラメータを読み込む手段を有し、第 1 の暗号化・復号化手段及び第 2 の暗号化・復号化手段 3 1 0 は、メモリデバイス ID と対向通信装置 ID を含むデータを暗号化・復号化する手段を有する。

【 0 0 1 4 】第 8 の発明において、対向通信装置 2 0 0 は、対向通信装置 2 0 0 間で、暗号化の第 2 のパラメータもしくは、第 2 の暗号化則を共有する第 2 の暗号化則共有手段と、第 2 の暗号化則共有手段において、共有されている第 2 のパラメータもしくは、第 2 の暗号化則で暗号化、復号化する第 3 の暗号化・復号化手段と、メモリデバイス ID を第 3 の暗号化・復号化手段で暗号化したデータを含むデータを、更に、第 1 の暗号化・復号化手段で暗号化して、メモリデバイス 1 0 0 に格納する暗号化データ格納制御手段と、暗号化格納制御手段によりメモリデバイス 1 0 0 に格納された暗号化データを読み取る暗号化データ読み取り手段と、暗号化データ読み取り手段により取得した暗号化データから、2 種類以上のメモリデバイス ID を照合する照合手段とを有する。

【0015】第9の発明において、照合手段は、暗号化データ読み取り手段により取得した暗号化データに、第1の暗号化・復号化手段を適用して特定したメモリデバイスIDと、同時に特定される該メモリデバイスIDが第3の暗号化・復号化手段で暗号化されている部分のデータについて更に、該第3の暗号化・復号化手段を適用して特定したメモリデバイスIDとを照合する手段を含む。

【0016】第10の発明は、照合手段において、メモリデバイスIDが照合できた場合には、暗号化データとメモリデバイスIDに対応するメモリデバイスIDを暗号化したデータ及び暗号化パラメータをメモリデバイス100に格納する第1の再格納手段を含む。

【0017】第11の発明において、対向通信装置200は、金額情報を含むカウンタ情報を有するデータと該データの暗号化情報を該メモリデバイス100に格納する暗号化情報格納制御手段と、暗号化情報格納制御手段によりメモリデバイス100に格納されたカウンタ情報及び暗号化情報を読み取る暗号化情報読み取り手段と、暗号化情報読み取り手段により取得した2種類以上のカウンタ情報を照合するカウンタ情報照合手段とを含む。

【0018】第12の発明において、カウンタ情報照合手段は、暗号化情報読み取り手段により取得したカウンタ情報と、暗号化情報を復号して、特定されたカウンタ情報とを照合する手段を含む。第13の発明は、カウンタ情報照合手段において、カウンタ情報が照合できた場合には、該カウンタ情報、メモリデバイスIDと該カウンタ情報を暗号化したデータ、及び暗号化パラメータを格納する第2の再格納手段を含む。

【0019】上記の第1、第2の発明は、メモリデバイスに当該メモリデバイスのID（メモリデバイスID）を含むデータを書き込む際に、パラメータを有する暗号化則を適用してデータを暗号化し、当該暗号化データとパラメータをメモリデバイスIDに対応する当該メモリデバイスに書き込む。さらに、メモリデバイスからデータを読み込む際には、メモリデバイスからデータを読み込んで、暗号化データとパラメータを特定し、パラメータを有する暗号化則を適用してデータを復号することにより、共有鍵を用いずに各メモリデバイス固有のパラメータを用いて暗号化・復号化が可能となる。

【0020】第3の発明は、第1、第2の発明におけるメモリデバイスIDを含むデータの書き込み、読み込みの代わりに、対向通信装置がメモリデバイスIDと対向通信装置IDを含むデータの書き込み、読み込みを行うことにより、さらに複雑化した暗号化・復号化が可能となる。

【0021】第4の発明は、第1、第2の発明における方法に加えて、対向通信装置間で暗号化の別のパラメータを共有し、対向通信装置がメモリデバイスIDを別のパラメータで暗号化した情報を含めたデータを更に暗号

化して、メモリデバイスに書き込み、かつ、当該メモリデバイスから読み出して復号する。別のパラメータで暗号化された部分については、更に復号し、この2つの手順により取得したメモリデバイスIDを照合することにより、照合できない場合には不正であると判定することが可能となる。

【0022】第5の発明は、第1、第2の発明における方法に加えて、対向通信装置が金額情報等のカウンタ情報をメモリデバイスに書き込むと共に、カウンタ情報を含むデータを暗号化して書き込み、かつ、メモリデバイスから読み出して復号し、2つのカウンタ情報を照合することにより、照合できない場合には不正であると判定することが可能となる。

【0023】第6の発明は、対向通信装置とセンタ装置に、パラメータに応じて暗号化則を変化させてデータを暗号化、復号する手段を設け、メモリデバイスのメモリデバイスIDを含むデータを暗号化したデータと、暗号化のパラメータをメモリデバイス内に書き込むことにより、対向通信装置とセンタ装置においてメモリデバイス固有の鍵情報を取得し、暗号化・復号化が可能となる。

【0024】第7の発明は、第6の発明におけるメモリデバイスIDを含むデータを暗号化したデータと暗号化パラメータをメモリデバイスに書き込む代わりに、メモリデバイスIDと対向装置IDを含むデータを暗号化したデータと、暗号化パラメータをメモリデバイス内に記録することにより、複雑化した暗号化・復号化が必要となるため、容易に復号化して悪用することが困難となる。

【0025】第8、第9及び第10の発明は、第6の発明に加え、対向通信装置に対向通信装置間で暗号化のための別のパラメータを共有させることにより、対向通信装置及びセンタ装置に、メモリデバイスのIDを別のパラメータで暗号化及び復号化する手段を設け、さらに、2種類のメモリデバイスIDを照合することにより、照合できない場合には、不正であるものと判定することができる。

【0026】第11、第12及び第13の発明は、第6の発明に加え、対向通信装置にメモリデバイスに金額情報等のカウンタ情報を書き込む手段と、カウンタ情報を含むデータを暗号化して書き込む手段と、メモリデバイスからデータを読み出して復号し、カウンタ情報を特定する手段と、暗号化されたカウンタ情報を復号し、特定されているカウンタ情報の2種類のカウンタ情報を照合する手段を設けることにより、2つのカウンタ情報を照合して、照合できない場合には、不正であるものと判定することができる。

【0027】このように、本発明は、各メモリデバイスに、必要情報の暗号化データに加え、当該各メモリデバイス固有の暗号化パラメータを含めて記録できるので、各対向通信装置及びセンタ装置が暗号化パラメータから

各メモリデバイス固有の鍵情報を導出することができる。このため、当該鍵情報を用いて、暗号化、復号化が実施できる。これにより、メモリデバイスに演算能力やデータ記憶量等の計算リソースを過大に持たせることなく、当該メモリデバイスのID情報等を各メモリデバイス毎に異なる暗号化パラメータで暗号化して通知することができ、不正情報通知等を受け難いID管理システムが実現できる。

【0028】さらに、メモリデバイスに、当該メモリデバイスのID情報を別のパラメータで暗号化したデータに加えて暗号化して書き込み、当該メモリデバイスから読み出して復号する時に、2種のID情報を照合することにより、暗号化、復号化処理の正当性を推定することができる。

【0029】また、メモリデバイスに金額情報等のカウンタ情報を書き込むと共に、カウンタ情報を含むデータを暗号化して書き込み、メモリデバイスから読み出して2つのカウンタ情報を復号した結果、2つのカウンタ情報を照合することにより、カウンタ情報の改ざんを抑止できる。

【0030】

【発明の実施の形態】図3は、本発明の第1の使用装置ID伝送システムの構成を示す。同図に示すシステムは、メモリデバイス100、対向通信装置200、センタ装置300、及び対向通信装置200とセンタ装置300を接続する通信回線設備400より構成される。

【0031】同図に示す例は、メモリデバイス100と対向通信装置200は、直接交信する形態の例である。対向通信装置200が、メモリデバイス100にコマンドを発行すると、メモリデバイス100が、応答し、アクセスを許可する。これにより、対向通信装置200は、コマンドを介してメモリデバイス100にデータを書き込むことができる。

【0032】図4は、本発明の使用装置ID伝送システムの各装置構成を示す。メモリデバイス100は、対向通信装置200からのコマンドに従いデータを記憶するデータ記憶部110と、対向通信装置200からのコマンドに従い、データ書き込み要求または、読み込み要求に応じて、データ記憶部110を制御して、対向通信装置200からの要求に対応する制御を行うデータ制御部120より構成される。

【0033】対向通信装置200は、メモリデバイス100にデータを書き込むコマンドを発行し、データ転送を行うデータ格納制御部210、メモリデバイス100からデータを取得するコマンドを発行し、データの読み込みを行うデータ読出制御部220、パラメータに応じて暗号化則を変化させてデータを暗号化・復号化する暗号化・復号化部230、データを暗号化・復号化するための規則である暗号化則240、及びセンタ装置300と情報交信する通信制御部250、暗号化・復号化部2

30により暗号化・復号化されたデータを格納する暗号化・復号化データ格納部260、復号化された2種類以上のメモリデバイスIDや金額情報等のカウンタ情報を照合する照合部270より構成される。

【0034】センタ装置300は、パラメータに応じて暗号化則を変化させてデータを暗号化・復号化する暗号化・復号化部310、暗号化・復号化部310により参照される暗号化則320、対向通信装置200と情報を交信する通信制御部330、暗号化・復号化された情報、または、転送されたデータからメモリデバイスID、対向通信装置IDを認識する認識部340から構成される。

【0035】上記の構成において、対向通信装置200が最初にデータを書き込む装置である場合には、暗号化・復号化部230において、書き込み対象のメモリデバイス100のメモリデバイスIDを含むデータを、パラメータを有する暗号化則240で暗号化してデータ格納制御部210に転送する。これにより、データ格納制御部210は、当該暗号化データをメモリデバイス100に転送する。メモリデバイス100のデータ制御部120は、当該暗号化データをデータ記憶部110に格納する。

【0036】また、対向通信装置200が上記の対向通信装置以降（ n 番目： $n \geq 2$ ）にメモリデバイス100に書き込みを行う装置である場合には、対向通信装置200のデータ読出制御部220がメモリデバイス100に読出用のコマンドを転送する。メモリデバイス100のデータ制御部120が当該コマンドを受け取ると、データ記憶部110からパラメータと暗号化データを抽出し、対向通信装置200のデータ読出制御部220に転送する。これにより、転送されたデータは、読出制御部220から暗号化・復号化部230に転送される。暗号化・復号化部230は、暗号化データを抽出し、暗号化則240を用いて復号して、メモリデバイス100のメモリデバイスIDを特定する。更に、当該メモリデバイスIDを暗号化則240を用いて暗号化して、当該暗号化則240のうち、暗号化に用いられたパラメータと暗号化されたメモリデバイスIDを暗号化データとして、データ格納制御部210を介してメモリデバイス100に転送する。これにより、当該データがメモリデバイス100のデータ制御部120を介してデータ記憶部110に格納される。

【0037】さらに、本発明では、最初にメモリデバイス100に書き込みを行う対向通信装置200がメモリデバイスIDと自装置200の対向通信装置IDを暗号化則240を用いて暗号化・復号化部230で暗号化して、メモリデバイス100のデータ記憶部110に書き込む。さらに、 n 番目にメモリデバイス100に書き込みを行う対向通信装置200は、メモリデバイス100から暗号化データを読み出して、暗号化則240を用い

て暗号化・復号化部 230 で当該データを復号し、メモリデバイス ID と $n-1$ 番目または、 $n-i$ ($n > i \geq 2$) 番目にメモリデバイス 100 に書き込みを行った対向通信装置 200 の対向通信装置 ID を特定し、暗号化則 240 の暗号化パラメータを用いて、対向通信装置 ID とメモリデバイス ID を暗号化・復号化部 230 で暗号化して、データ格納制御部 210 を介してメモリデバイス 100 のデータ記憶部 110 に書き込む。

【0038】さらに、本発明では、対向通信装置 200 は、上記のようにして得られたメモリデバイス ID

(A) を暗号化・復号化データ格納部 260 に格納しておくと共に、当該メモリデバイス ID を暗号化則 240 の他のパラメータで暗号化し、当該暗号化されたメモリデバイス ID を復号したメモリデバイス ID (B) を暗号化・復号化データ格納部 260 に格納する。これにより、最初に格納されたメモリデバイス ID (A) と次に格納されたメモリデバイス ID (B) を照合部 270 に転送し、当該照合部 270 で両者が一致するかを調べる。

【0039】さらに、本発明では、対向通信装置 200 (1) は、金額情報等のカウンタ情報を含むデータと暗号化情報をメモリデバイス 100 のデータ格納部 110 に書き込み、それ以降にメモリデバイス 100 に書き込みを行う対向通信装置 (n) が、メモリデバイス 100 からデータを読み込んで、カウンタ情報と暗号化情報を抽出して暗号化・復号化データ格納部 260 に格納しておき、当該暗号化情報を復号し、カウンタ情報を特定し、暗号化・復号化データ格納部 260 に格納されているカウンタ情報と復号されたカウンタ情報を照合部 270 で照合する。

【0040】また、センタ装置 300 は、メモリデバイス 100 のデータ記憶部 110 に書き込まれていたデータをそのままの形式、または、対向通信装置 200 により変形された形式で、通信制御部 330 を介して取得し、暗号化データを暗号化則 320 を用いて暗号化・復号化部 310 で復号して、復号されたデータを認識部 340 に転送し、データ認識部 340 でメモリデバイス 100 を特定する。

【0041】また、センタ装置 300 は、暗号化データに対向通信装置 ID も含まれている場合には、暗号化・復号化部 310 で復号してメモリデバイス 100 と対向通信装置 200 を特定する。また、上記の構成は、メモリデバイス 100 と対向通信装置 200 が直接交信する構成であるが、図 5 に示すように、通信回線設備 400 を介してメモリデバイス 100 と対向通信装置 200 が交信する形態がある。

【0042】図 5 に示す構成は、対向通信装置は、物理的な対向通信装置 201 と論理的な対向通信装置 202 があり、物理的な対向通信装置 201 は単なる中継装置としてのみ働き、前述の対向通信装置が行う処理は、全

て論理的な対向通信装置 202 が行う。論理的な対向通信装置 202 とセンタ装置 300 は、通信回線設備 400 を介して接続されており、相互に通信可能である。

【0043】

【実施例】以下、図面と共に本発明の実施例を説明する。

【第 1 の実施例】第 1 の実施例として、第 1 の対向通信装置がメモリデバイスに暗号化されたデータ (メモリデバイス ID) を書き込み、第 2 の対向通信装置が第 1 の対向通信装置により書き込まれたデータを復号し、さらに、独自に暗号化したデータをメモリデバイスに書き込み、センタ装置において、対向通信装置から渡されたデータを特定する例を示す。

【0044】図 6 は、本発明の第 1 の実施例の処理の概要を示す。同図において、メモリデバイス 100 a と最初にやり取りする対向通信装置 200 a は、メモリデバイス 100 a の ID を含むデータを暗号化したデータ α とその暗号化パラメータ α を、メモリデバイス 100 a の指定レコード位置に書き込む。以降、メモリデバイス 100 a とやり取りする対向通信装置 200 b は、メモリデバイス 100 a から暗号化パラメータ α を読み取り、暗号化データ復号則を推定する。暗号化パラメータから復号則を導出する方法は、正規の対向通信装置間で共有している。

【0045】さらに、メモリデバイス 100 a から暗号化データ α を読み取り、これを復号してメモリデバイス ID を取得する。センタ装置 300 は、対向通信装置 200 b から暗号化パラメータ α を読み取り、暗号化復号則を推定する。暗号化パラメータから復号則を導出する方法は、正規の対向通信装置及びセンタ装置間で共有している。

【0046】さらに、センタ装置 300 は、対向通信装置 200 b から暗号化データ α を読み取り、これを復号してメモリデバイス ID を取得する。図 7 は、本発明の第 1 の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作を示すフローチャートである。

【0047】ステップ 101) 対向通信装置 200 a は、メモリデバイス 100 a を起動させる。

ステップ 102) メモリデバイス 100 a が起動する。

ステップ 103) 対向通信装置 200 a は、データを書き込むメモリデバイス 100 a のメモリデバイス ID を特定する。

【0048】ステップ 104) 対向通信装置 200 a が書き込みデータを暗号化するための暗号化パラメータ α を特定する。

ステップ 105) 対向通信装置 200 a の暗号化・復号化部 230 は、メモリデバイス 100 のメモリデバイス ID を含むデータを暗号化則 240 の暗号化パラメータ α を用いて暗号化する。

【0049】ステップ106) 対向通信装置200aのデータ格納制御部210は、暗号化時に使用した暗号化パラメータ α をメモリデバイス100aのデータ記憶部110の指定レコード位置に書き込むためのコマンドをメモリデバイス100aに送信する。

【0050】ステップ107) メモリデバイス100aのデータ制御部120は、対向通信装置200aから暗号化パラメータ α の書き込みのコマンドを受け取ると、データ記憶部110の指定レコード位置に、暗号化パラメータ α を書き込む。

ステップ108) さらに、対向通信装置200aは、暗号化された暗号化データ α をメモリデバイス100aのデータ記憶部110の指定レコード位置に書き込むためのコマンドをメモリデバイス100aに送信する。

【0051】ステップ109) メモリデバイス100aのデータ制御部120は、対向通信装置200aから暗号化データ α の書き込みのコマンドを受け取ると、データ記憶部120の指定レコード位置に、暗号化データ α を書き込む。図8は、本発明の第1の実施例のメモリデバイスと対向通信装置が2回目以降にやり取りする際の動作のフローチャートである。

【0052】ステップ110) 対向通信装置200bがメモリデバイス100aを起動する。

ステップ111) メモリデバイス100aが起動する。

ステップ112) 対向通信装置200bは、メモリデバイス100aのデータ記憶部110に格納されている暗号化パラメータ α を読み取るコマンドをデータ読出制御部220から発行する。

【0053】ステップ113) メモリデバイス100aのデータ制御部120は、対向通信装置200bに対して、データ記憶部110からの暗号化パラメータ α の読み出しを許可する。

ステップ114) 対向通信装置200bのデータ読出制御部220は、メモリデバイス100aのデータ記憶部110から暗号化パラメータ α を読み取る。

【0054】ステップ115) 次に、対向通信装置200bのデータ読出制御部220は、メモリデバイス100aに対して暗号化データ α を読み出すコマンドを送信する。

ステップ116) メモリデバイス100aのデータ制御部120は、受信した読み出しコマンドに対する読み出しを許可する。

【0055】ステップ117) 対向通信装置200bのデータ読出制御部220は、メモリデバイス100aから暗号化データ α を読み取り、暗号化・復号化データ格納部260に格納する。

ステップ118) 対向通信装置200bのデータ読出制御部220により取得し、暗号化・復号化データ格納部260に格納されている暗号データ α を暗号化・復号

化部230により復号する。

【0056】ステップ119) 復号された暗号化データ α からメモリデバイス100aのメモリデバイスIDを特定する。なお、上記のステップ118において暗号化データを復号化する際に用いる復号化パラメータは、正規の対向通信装置間(200a, 200b)で共有しているものとする。

【0057】さらに、図7に示す動作と同様に、対向通信装置200bが暗号化パラメータ β 、暗号化データ β をメモリデバイス100aに転送し、メモリデバイス100aにおいて、当該暗号化パラメータ β と暗号化データ β をデータ記憶部110に格納する。

【0058】図9は、本発明の第1の実施例の対向通信装置とセンタ装置の動作のフローチャートである。

ステップ120) センタ装置300は、対向通信装置200bを起動させる。

【0059】ステップ121) 対向通信装置200bが起動する。

ステップ122) センタ装置300は、暗号化パラメータ α を読み取るコマンドを通信制御部330を介して対向通信装置200bに発行する。

ステップ123) 対向通信装置200bは、通信制御部250を介して当該コマンドを受信すると、暗号化・復号化データ格納部260に格納されている暗号化データ α を通信制御部250を介してセンタ装置300に送信する。

【0060】ステップ124) センタ装置300は、暗号化データ α を通信制御部330を介して読み取り、暗号化・復号化部310に転送する。

ステップ125) 暗号化・復号化部310は、暗号化データを暗号化則320の暗号パラメータを用いて復号し、復号した結果を認識部340に転送する。

【0061】ステップ126) 認識部340は、復号した結果よりメモリデバイスIDを特定する。

〔第2の実施例〕次に、第2の実施例として、第1の対向通信装置がメモリデバイスに暗号化されたデータ(メモリデバイスID、対向通信装置ID)を書き込み、第2の対向通信装置が第1の対向通信装置により書き込まれたデータを復号し、さらに、独自に暗号化したデータ(メモリデバイスID、対向通信装置ID)をメモリデバイスに書き込み、センタ装置において、対向通信装置から渡されたデータ(メモリデバイスID、対向通信装置ID)を特定する例を示す。

【0062】図10は、本発明の第2の実施例の処理の概要を示す図である。メモリデバイス100aと最初にやり取りする対向通信装置200aは、当該メモリデバイス100aのIDと対向通信装置IDを含むデータを暗号化したデータ γ と、暗号化パラメータ γ を、メモリデバイス100aの指定レコード位置に書き込む。以降、メモリデバイス100aとやり取りする対向通信装

置 2 0 0 b は、メモリデバイス 1 0 0 a から暗号化パラメータを読み取り、暗号化データ復号則を推定する。なお、暗号化パラメータから復号則を導出する方法は、正規の対向通信装置間で共有している。

【0 0 6 3】さらに、対向通信装置 2 0 0 b は、メモリデバイス 1 0 0 a から暗号化データを読み取り、これを復号してメモリデバイス ID と前にやり取りしていた対向通信装置 ID を取得する。その後、メモリデバイス 1 0 0 a の ID と対向通信装置 ID を含むデータを暗号化したデータ δ とその暗号化パラメータ δ を、メモリデバイス 1 0 0 a の指定レコード位置に書き込む。

【0 0 6 4】センタ装置 3 0 0 は、対向通信装置 2 0 0 b から暗号化パラメータを読み取り、暗号化データ復号則を推定する。なお、暗号化パラメータから復号則を導出する方法は、正規の対向通信装置及びセンタ装置間で共有している。さらに、センタ装置 3 0 0 は、対向通信装置 2 0 0 b から暗号化データを読み取り、これを復号してメモリデバイス ID と前にやり取りがあった対向通信装置 ID を取得する。

【0 0 6 5】図 1 1 は、本発明の第 2 の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作を示すフローチャートである。

ステップ 2 0 1) 対向通信装置 2 0 0 a は、メモリデバイス 1 0 0 a を起動する。

【0 0 6 6】ステップ 2 0 2) メモリデバイス 1 0 0 a が起動する。

ステップ 2 0 3) 対向通信装置 2 0 0 a は、メモリデバイス 1 0 0 a のメモリデバイス ID を特定する。

ステップ 2 0 4) 対向通信装置 2 0 0 a は、暗号化則 2 4 0 から暗号化パラメータを特定する。

【0 0 6 7】ステップ 2 0 5) 対向通信装置 2 0 0 a は、メモリデバイス ID と自対向通信装置 2 0 0 a の対向通信装置 ID を含むデータを暗号化・復号化部 2 3 0 において暗号化パラメータを用いて暗号化する。

ステップ 2 0 6) 対向通信装置 2 0 0 a は、暗号化パラメータをデータ格納制御部 2 1 0 を介してメモリデバイス 1 0 0 a に書き込むためのコマンドを送信する。

【0 0 6 8】ステップ 2 0 7) メモリデバイス 1 0 0 a は、暗号化パラメータをデータ記憶部 1 1 0 に書き込む。

ステップ 2 0 8) 対向通信装置 2 0 0 a は、対向通信装置 ID を含む暗号化データ δ をメモリデバイス 1 0 0 a に書き込むためのコマンドを送信する。

【0 0 6 9】ステップ 2 0 9) メモリデバイス 1 0 0 a は、暗号化データをデータ記憶部 1 1 0 に書き込む。図 1 2 は、本発明の第 2 の実施例のメモリデバイスと対向通信装置が 2 回目以降にやり取りする際の動作のフローチャートである。

【0 0 7 0】ステップ 2 1 0) 対向通信装置 2 0 0 b がメモリデバイス 1 0 0 a を起動する。

ステップ 2 1 1) メモリデバイス 1 0 0 a が起動する。

ステップ 2 1 2) 対向通信装置 2 0 0 b は、メモリデバイス 1 0 0 a のデータ記憶部 1 1 0 に格納されている暗号化パラメータを読み取るコマンドをデータ読出制御部 2 2 0 から発行する。

【0 0 7 1】ステップ 2 1 3) メモリデバイス 1 0 0 a のデータ制御部 1 2 0 は、対向通信装置 2 0 0 b に対してデータ記憶部 1 1 0 からの暗号化パラメータの読み出しを許可する。

ステップ 2 1 4) 対向通信装置 2 0 0 b のデータ読出制御部 2 2 0 は、メモリデバイス 1 0 0 a のデータ記憶部 1 1 0 から暗号化パラメータを読み取る。

【0 0 7 2】ステップ 2 1 5) 次に、対向通信装置 2 0 0 b のデータ読出制御部 2 2 0 は、メモリデバイス 1 0 0 a に対して暗号化データを読み出すコマンドを送信する。

ステップ 2 1 6) メモリデバイス 1 0 0 a のデータ制御部 1 2 0 は、受信した読み出したコマンドに対する読み出しを許可する。

【0 0 7 3】ステップ 2 1 7) 対向通信装置 2 0 0 b のデータ読出制御部 2 2 0 は、メモリデバイス 1 0 0 a から暗号化データを読み取り、暗号化・復号化データ格納部 2 6 0 に格納する。

ステップ 2 1 8) 対向通信装置 2 0 0 b のデータ読出制御部 2 2 0 により取得し、暗号化・復号化データ格納部 2 6 0 に格納されている暗号データを暗号化・復号化部 2 3 0 により復号する。

【0 0 7 4】ステップ 2 1 9) 復号された暗号化データからメモリデバイス 1 0 0 a のメモリデバイス ID と対向通信装置 ID を含むデータを特定する。

ステップ 2 2 0) 対向通信装置 2 0 0 b は、メモリデバイス ID と対向通信装置 ID を含むデータを、暗号化則 2 4 0 の暗号化パラメータ δ を用いて暗号化・復号化部 2 3 0 で暗号化する。

【0 0 7 5】ステップ 2 2 1) 対向通信装置 2 0 0 b は、暗号化・復号化部 2 3 0 で用いられた暗号化パラメータ δ をメモリデバイス 1 0 0 a に書き込むためのコマンドをデータ格納制御部 2 1 0 を介して送信する。

ステップ 2 2 2) メモリデバイス 1 0 0 a は、データ記憶部 1 1 0 に暗号化パラメータ δ を書き込む。

【0 0 7 6】ステップ 2 2 3) 対向通信装置 2 0 0 b は、対向通信装置 ID を含む暗号化データ δ を書き込むコマンドをデータ格納制御部 2 1 0 を介して送信する。

ステップ 2 2 4) メモリデバイス 1 0 0 a は、暗号化データ δ をデータ記憶部 1 1 0 に書き込む。

【0 0 7 7】図 1 3 は、本発明の第 2 の実施例の対向通信装置とセンタ装置との動作のフローチャートである。

ステップ 2 3 0) センタ装置 3 0 0 は、相手の対向通信装置 2 0 0 b を起動する。

【0078】ステップ231) 対向通信装置200bが起動する。

ステップ232) センタ装置300は、暗号化パラメータを読み取るコマンドを通信制御部330から対向通信装置200bに発行する。

ステップ233) 対向通信装置200bは、暗号化・復号化データ格納部260に格納されている暗号化パラメータを通信制御部250を介してセンタ装置300に送信する。

【0079】ステップ234) センタ装置300は、対向通信装置200bから暗号化パラメータを受信し、暗号化データ復号則を推定する。なお、暗号化パラメータから復号則を導く方法は、正規の対向通信装置200及びセンタ装置300間で共有している。

【0080】ステップ235) センタ装置300は、暗号化データを読み取るコマンドを対向通信装置200bに通信制御部330から発行する。

ステップ236) 対向通信装置200bは、暗号化・復号化データ格納部260に格納されている暗号化データをセンタ装置300に送信する。

【0081】ステップ237) センタ装置300は、対向通信装置200bから暗号化データを受信する。

ステップ238) センタ装置300の暗号化・復号化部310は、暗号化データを復号し、復号結果を認識部340に転送する。

【0082】ステップ239) センタ装置300の認識部340は、復号結果からメモリデバイスID(100a)と対向通信装置ID(200b)を特定する。

【第3の実施例】次に、第3の実施例を説明する。

【0083】図14は、本発明の第3の実施例の処理の概要を示す。本実施例は、全ての対向通信装置200に暗号化則と暗号化パラメータAを共有させておき、メモリデバイス100aと最初のやり取りする対向通信装置200aが、まず、メモリデバイスのIDを含むデータに暗号化パラメータAを適用して暗号化し、次に、暗号化データとメモリデバイスIDを含むデータに暗号化パラメータBを適用して更に暗号化し、当該暗号化データBと暗号化パラメータBをメモリデバイス100aの指定レコード位置に格納する。以降、メモリデバイス100aとやり取りする対向通信装置200bは、メモリデバイス100aから暗号化データB及び暗号化パラメータBを読み取り、暗号化データ復号則を推定する。推定復号則を暗号化データBに適用し、メモリデバイスIDを含むデータや当該暗号化データBを特定する。特定した暗号化データについては、暗号化パラメータAを適用して更に復号し、メモリデバイスIDを特定する。

【0084】その結果、当該メモリデバイス100aのメモリデバイスIDが2度特定されたことになるので、2種のメモリデバイスIDが等しく得られたかどうか、2種のデータを照合する。その結果、照合できたとき、

対向通信装置200bは、メモリデバイス100aのメモリデバイスIDを取得する。

【0085】図15は、本発明の第3の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作のフローチャートである。

ステップ301) 対向通信装置200aは、メモリデバイス100aを起動する。

【0086】ステップ302) メモリデバイス100aが起動する。

ステップ303) 対向通信装置200aは、メモリデバイス100aのメモリデバイスIDを特定する。

ステップ304) 対向通信装置200aは、暗号化則240から暗号化パラメータAを特定する。

【0087】ステップ305) 対向通信装置200aの暗号化・復号化部230は、ステップ303で特定したメモリデバイスIDを含むデータを暗号化パラメータAを用いて暗号化し、当該暗号化結果を暗号化データAとする。

ステップ306) 対向通信装置200aは、暗号化則240から暗号化パラメータBを特定する。

【0088】ステップ307) 上記のメモリデバイスIDと、暗号化データAを暗号化パラメータBを用いて更に暗号化し、当該暗号化結果を暗号化データBとする。

ステップ308) 対向通信装置200aは、データ格納制御部210を介して暗号化パラメータBをメモリデバイス100aに転送する。

【0089】ステップ309) メモリデバイス100aのデータ制御部120は、対向通信装置200aから取得した暗号化パラメータBをデータ記憶部110に格納する。

ステップ310) 対向通信装置200aは、暗号化データBを書き込むコマンドをデータ格納制御部210からメモリデバイス100aに転送する。

【0090】ステップ311) メモリデバイス100aのデータ制御部120は、対向通信装置200aから取得した暗号化データBをデータ記憶部110に格納する。図16は、本発明の第3の実施例のメモリデバイスと対向通信装置が2回目以降にやり取りする際の動作のフローチャートである。

【0091】ステップ320) 対向通信装置200bがメモリデバイス100aを起動する。

ステップ321) メモリデバイス100aが起動する。

ステップ322) 対向通信装置200bは、暗号化パラメータBを読み取るコマンドをデータ読出制御部220からメモリデバイス100aに発行する。

【0092】ステップ323) メモリデバイス100aのデータ制御部120は、データ記憶部110に格納されている暗号化パラメータBを読み出し可能とする。

ステップ 324) 対向通信装置 200b のデータ読出制御部 220 は、暗号化パラメータ B をデータ記憶部 110 から読み取る。

【0093】ステップ 325) 対向通信装置 200b は、暗号化データ B を読み取るコマンドをデータ読出制御部 220 からメモリデバイス 100a に発行する。

ステップ 326) メモリデバイス 100a のデータ制御部 120 は、データ記憶部 110 に格納されている暗号化データ B を読み出し可能とする。

【0094】ステップ 327) 対向通信装置 200b のデータ読出制御部 220 は、暗号化データ B をデータ記憶部 110 から読み取る。

ステップ 328) 対向通信装置 200b の取得した暗号化データ B を暗号化パラメータ B で復号する。

【0095】ステップ 329) 対向通信装置 200b は、復号結果からメモリデバイス ID、暗号化データを特定し、暗号化・復号化データ格納部 260 に格納する。

ステップ 330) 各対向通信装置 200 で共有している暗号化パラメータ A を特定する。

【0096】ステップ 331) 対向通信装置 200b は、ステップ 327 で取得した暗号化データ B を暗号化パラメータ A で復号する。

ステップ 332) 対向通信装置 200b は、復号結果からメモリデバイス ID を特定する。

【0097】ステップ 333) 対向通信装置 200b の照合部 270 は、ステップ 329 において、暗号化・復号化データ格納部 260 に格納されているメモリデバイス ID とステップ 332 で特定されたメモリデバイス ID を照合し、照合できない場合にはステップ 334 に移行し、照合できた場合には、ステップ 335 に移行する。

【0098】ステップ 334) 照合失敗の所定の処理を行い、処理を終了する。

ステップ 335) 対向通信装置 200b の暗号化・復号化部 2230 は、メモリデバイス ID と上記暗号化データ B を含むデータを更に暗号化する。

ステップ 336) 対向通信装置 200b のデータ格納制御部 210 は、暗号化パラメータ B をメモリデバイス 100a のデータ格納部 110 に格納するコマンドをメモリデバイス 100a に送出する。

【0099】ステップ 337) メモリデバイス 100a は、データ格納部 110 に暗号化パラメータ B を格納する。

ステップ 338) 対向通信装置 200b は、メモリデバイス 100a に暗号化データを書き込むコマンドをデータ格納制御部 210 から発行する。

【0100】ステップ 339) メモリデバイス 100a は、データ記憶部 110 に暗号化データを書き込む。

【第 4 の実施例】図 17 は、本発明の第 4 の実施例の処

理の概要を示す図である。

【0101】メモリデバイス 100a と最初のやり取りする対向通信装置 200a は、メモリデバイス 100a のメモリデバイス ID とカウンタ情報を含むデータを暗号化した暗号化データと当該暗号化パラメータ及びカウンタ情報をメモリデバイス 100a のデータ記憶部 110 に書き込む。

【0102】以降、メモリデバイス 100a とやり取りする対向通信装置 200b は、カウンタ情報をメモリデバイス 100a から読み取ると共に、暗号化パラメータを読み取り、暗号化データ復号則を推定する。暗号化パラメータから復号則を導出する方法は、対向通信装置 200 間で共有している。更に、メモリデバイス 100a から暗号化データを読み取り、これを復号して、メモリデバイス 100a のメモリデバイス ID とカウンタ情報を特定する。

【0103】その結果、カウンタ情報が 2 度特定されたことになるので、2 種のカウンタ情報が等しく得られたかどうか、2 種のデータを照合する。照合の結果、照合できた場合には、対向通信装置 200b は、カウンタ情報が正当なものであると見なして取得する。

【0104】その後、対向通信装置 200b は、必要であれば、カウンタ情報を更新し、メモリデバイス 100a のメモリデバイス ID とカウンタ情報を含むデータを暗号化したデータと当該暗号化パラメータ及びカウンタ情報をメモリデバイス 100a のデータ記憶部 110 に格納する。

【0105】図 18 は、本発明の第 4 の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作を示すフローチャートである。

ステップ 401) 対向通信装置 200a は、メモリデバイス 100a を起動する。

【0106】ステップ 402) メモリデバイス 100a が起動する。

ステップ 403) 対向通信装置 200a は、メモリデバイス ID を特定する。

ステップ 404) 対向通信装置 200a は、カウンタ情報を特定する。

【0107】ステップ 405) 対向通信装置 200a は、暗号化パラメータを特定する。

ステップ 406) 対向通信装置 200a は、メモリデバイス ID とカウンタ情報を含むデータを暗号化して、暗号化データとする。

【0108】ステップ 407) 対向通信装置 200a のデータ格納制御部 210 は、カウンタ情報をメモリデバイス 100a のデータ記憶部 110 に格納するためのコマンドを送信する。

ステップ 408) メモリデバイス 100a のメモリデバイス 100a のデータ記憶部 110 は、対向通信装置 200a から転送されたカウンタ情報を書き込む。

【0109】ステップ409) 対向通信装置200aは、暗号化パラメータをメモリデバイス100aのデータ記憶部110に書き込むコマンドを送信する。

ステップ410) メモリデバイス100aのメモリデバイス100aのデータ記憶部110は、対向通信装置200aから転送された暗号化パラメータを書き込む。

【0110】ステップ411) 対向通信装置200aは、暗号化データをメモリデバイス100aのデータ記憶部110に書き込むコマンドを送信する。

ステップ412) メモリデバイス100aのメモリデバイス100aのデータ記憶部110は、対向通信装置200aから転送された暗号化データを書き込む。

【0111】図19は、本発明の第4の実施例のメモリデバイスと対向通信装置が2回目以降にやり取りする際の動作のフローチャートである。

ステップ420) 対向通信装置200bがメモリデバイス100aを起動する。

【0112】ステップ421) メモリデバイス100aが起動する。

ステップ422) 対向通信装置200bは、カウンタ情報を読み取るコマンドをデータ読出制御部220からメモリデバイス100aに発行する。

ステップ423) メモリデバイス100aのデータ制御部120は、データ記憶部110に格納されているカウンタ情報を読み出し可能とする。

【0113】ステップ424) 対向通信装置200bのデータ読出制御部220は、カウンタ情報をデータ記憶部110から読み取る。

ステップ425) 対向通信装置200bは、暗号化パラメータを読み取るコマンドをデータ読出制御部220からメモリデバイス100aに発行する。

【0114】ステップ426) メモリデバイス100aのデータ制御部120は、データ記憶部110に格納されている暗号化パラメータを読み出し可能とする。

ステップ427) 対向通信装置200bのデータ読出制御部220は、暗号化パラメータをデータ記憶部110から読み取る。

【0115】ステップ428) 対向通信装置200bは、暗号化データを読み取るコマンドをデータ読出制御部220からメモリデバイス100aに発行する。

ステップ429) メモリデバイス100aのデータ制御部120は、データ記憶部110に格納されている暗号化データを読み出し可能とする。

【0116】ステップ430) 対向通信装置200bのデータ読み出し制御部220は、暗号化データをデータ記憶部110から読み取る。

ステップ431) 対向通信装置200bの取得した暗号化データを暗号化パラメータで復号する。

【0117】ステップ432) 対向通信装置200b

は、復号結果からメモリデバイスID、カウンタ情報を特定し、暗号化・復号化データ格納部260に格納する。

ステップ433) 対向通信装置200bは、ステップ424において、メモリデバイス100aから取得したカウンタ情報と、ステップ431で復号されたカウンタ情報を照合し、照合できなかった場合には、ステップ434に以降し、照合できた場合にはステップ435に移行する。

10 【0118】ステップ434) 照合しなかった場合には、所定の照合不可処理を行い、処理を終了する。

ステップ435) 対向通信装置200bは、当該カウンタ情報を更新する。

ステップ436) 対向通信装置200bの暗号化・復号化部230は、メモリデバイス100aのメモリデバイスIDとカウンタ情報を含むデータを暗号化する。

【0119】ステップ437) 対向通信装置200bは、更新されたカウンタ情報をデータ記憶部110に書き込むためのコマンドをデータ格納制御部210を介してメモリデバイス100aに送信する。

20 ステップ438) メモリデバイス100aのデータ記憶部110は、更新されたカウンタ情報を格納する。

【0120】ステップ439) 対向通信装置200bは、暗号化パラメータを書き込むコマンドをデータ格納制御部210を介してメモリデバイス100aに送出する。

ステップ440) メモリデバイス100aのデータ記憶部110は、暗号化パラメータをデータ記憶部110に書き込む。

30 【0121】ステップ441) 対向通信装置200bは、暗号化データを書き込むコマンドをデータ格納制御部210を介してメモリデバイス100aに送出する。

ステップ442) メモリデバイス100aのデータ記憶部110は、暗号化データをデータ記憶部110に書き込む。

【0122】なお、本発明は、上記の実施例の限定されことなく、特許請求の範囲内で種々変更・応用が可能である。

【0123】

40 【発明の効果】上述のように、本発明の使用装置ID伝達方法及びシステムによれば、メモリデバイスに演算能力やデータ記憶量等の計算リソースを過大に持たせることなく、不正情報通知等を受け難いID管理システムが実現できる。

【0124】また、本発明によれば、照合処理を行うことにより、暗号化・復号化処理の正当性が推定でき、金額情報等のカウンタ情報の改ざんを防止することが可能である。

【図面の簡単な説明】

50 【図1】本発明の原理を説明するための図である。

【図 2】本発明の原理構成図である。

【図 3】本発明の第 1 の使用装置 ID 伝送システムの構成図である。

【図 4】本発明の使用装置 ID 伝送システムの各装置構成図である。

【図 5】本発明の第 2 の使用装置 ID 伝送システムの構成図である。

【図 6】本発明の第 1 の実施例の処理の概要を示す図である。

【図 7】本発明の第 1 の実施例のメモリデバイスと対向通信装置が最初のデータをやり取りする動作を示すフローチャートである。

【図 8】本発明の第 1 の実施例のメモリデバイスと対向通信装置が 2 回目以降にやり取りする際の動作のフローチャートである。

【図 9】本発明の第 1 の実施例の対向通信装置とセンタ装置との動作のフローチャートである。

【図 10】本発明の第 2 の実施例の処理の概要を示す図である。

【図 11】本発明の第 2 の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作のフローチャートである。

【図 12】本発明の第 2 の実施例のメモリデバイスと対向通信装置が 2 回目以降にやり取りする際の動作のフローチャートである。

【図 13】本発明の第 2 の実施例の対向通信装置とセンタ装置との動作のフローチャートである。

【図 14】本発明の第 3 の実施例の処理の概要を示す図である。

【図 15】本発明の第 3 の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作のフローチャートである。

【図 16】本発明の第 3 の実施例のメモリデバイスと対向通信装置が 2 回目以降にやり取りする際の動作のフローチャートである。

【図 17】本発明の第 4 の実施例の処理の概要を示す図である。

【図 18】本発明の第 4 の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作を示すフローチャートである。

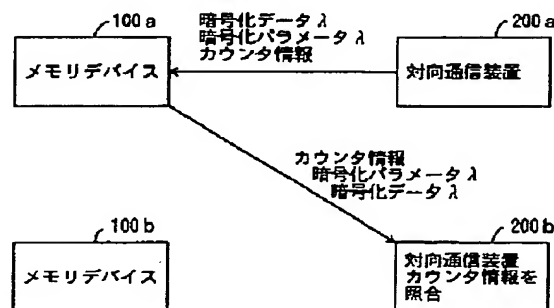
【図 19】本発明の第 4 の実施例のメモリデバイスと対向通信装置が 2 回目以降にやり取りする際の動作のフローチャートである。

【符号の説明】

100	メモリデバイス
110	データ記憶部、データ記憶手段
120	データ制御部
200	対向通信装置
201	物理的な対向通信装置
202	論理的な対向通信装置
210	データ格納制御部、書き込み手段
220	データ読出制御部、読み込み手段
230	暗号化・復号化部、第 1 の暗号化・復号化手段
240	暗号化則
250	通信制御部、センタ交信手段
260	暗号化・復号化データ格納部
270	照合部
300	センタ装置
310	暗号化・復号化部、第 2 の暗号化・復号化手段
320	暗号化則
330	通信制御部、対向通信装置交信手段
340	認識部、読み込み手段
400	通信回線設備

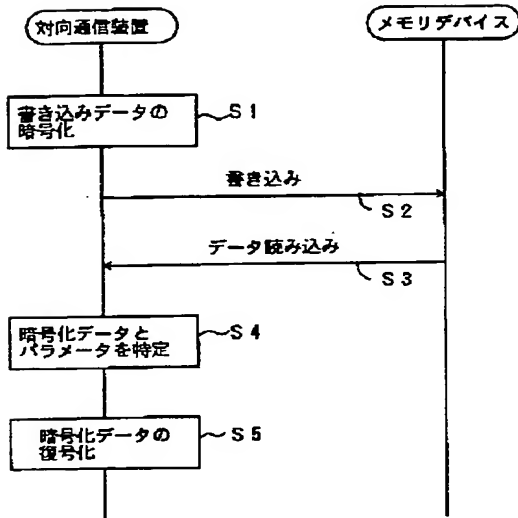
【図 17】

本発明の第 4 の実施例の処理の概要を示す図



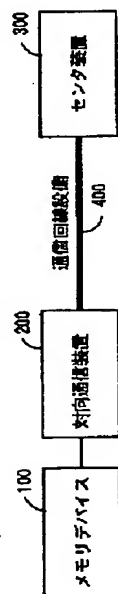
【 図 1 】

本発明の原理を説明するための図



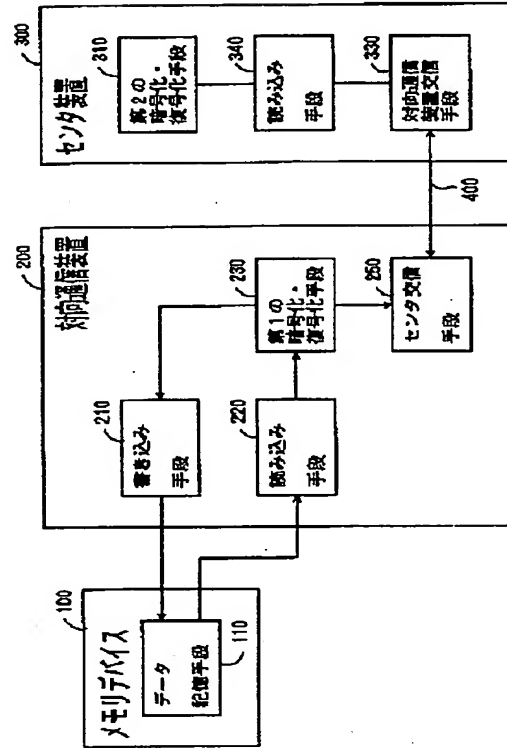
【 図 3 】

本発明の第1の使用装置 I D 伝送システムの構成図



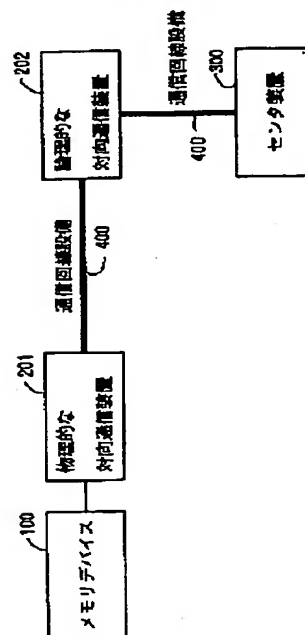
【 図 2 】

本発明の原理構成図



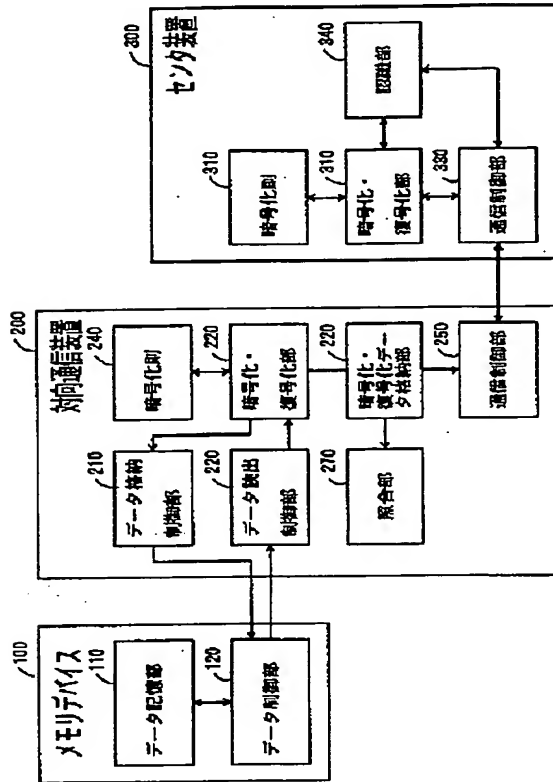
【 図 5 】

本発明の第2の使用装置 I D 伝送システムの構成図



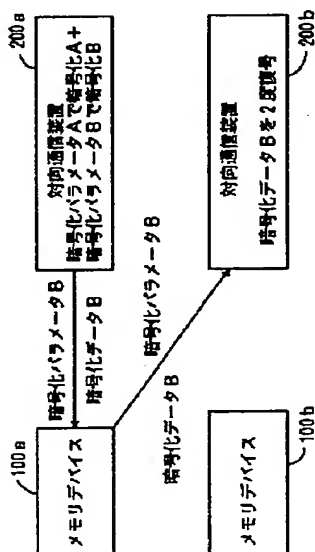
【 図 4 】

本発明の使用装置 I D 伝送システムの各装置構成図



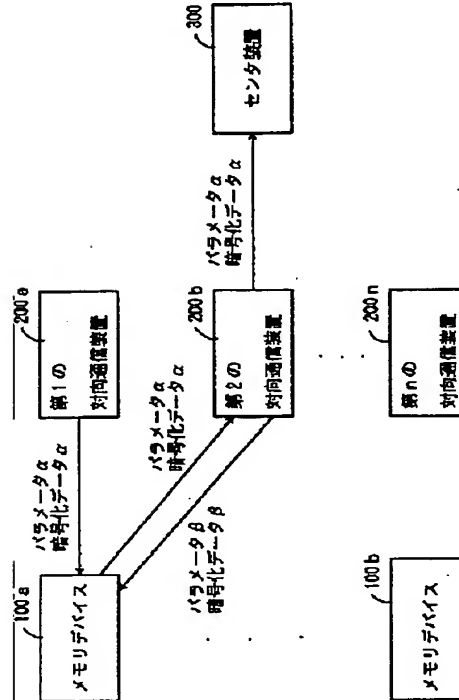
【 図 1 4 】

本発明の第 3 の実施例の処理の概要を示す図



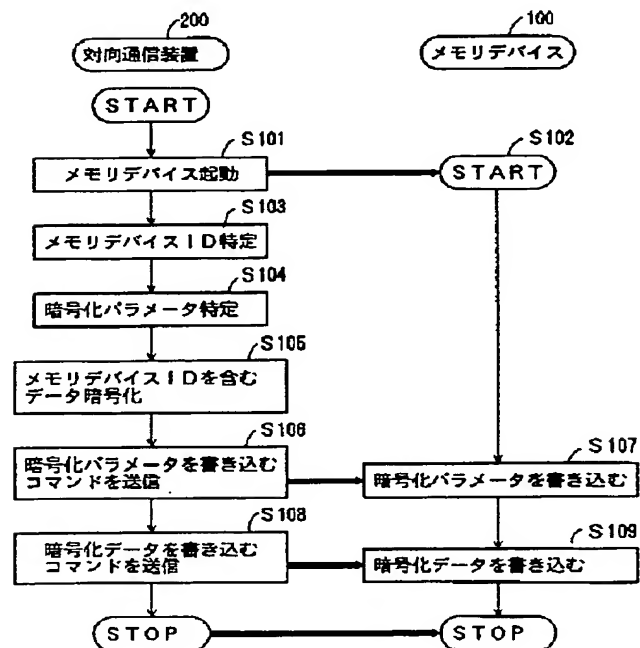
【 図 6 】

本発明の第 1 の実施例の処理の概要を示す図



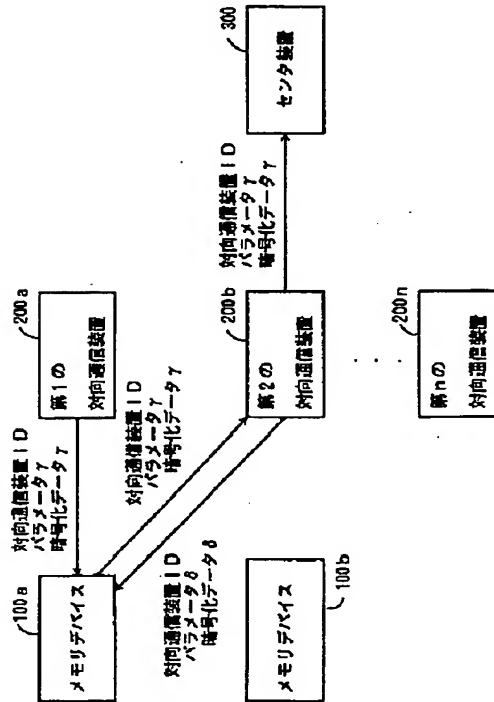
【 図 7 】

本発明の第 1 の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作を示すフローチャート



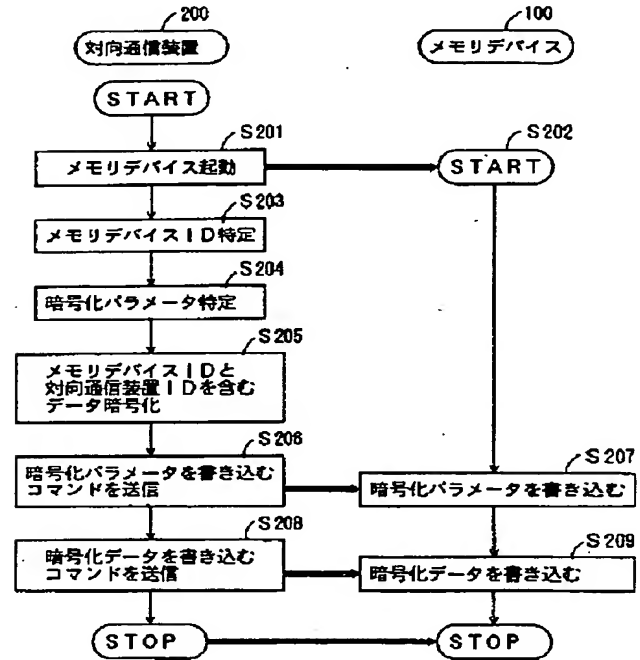
【 図 1 0 】

本発明の第2の実施例の処理の概要を示す図



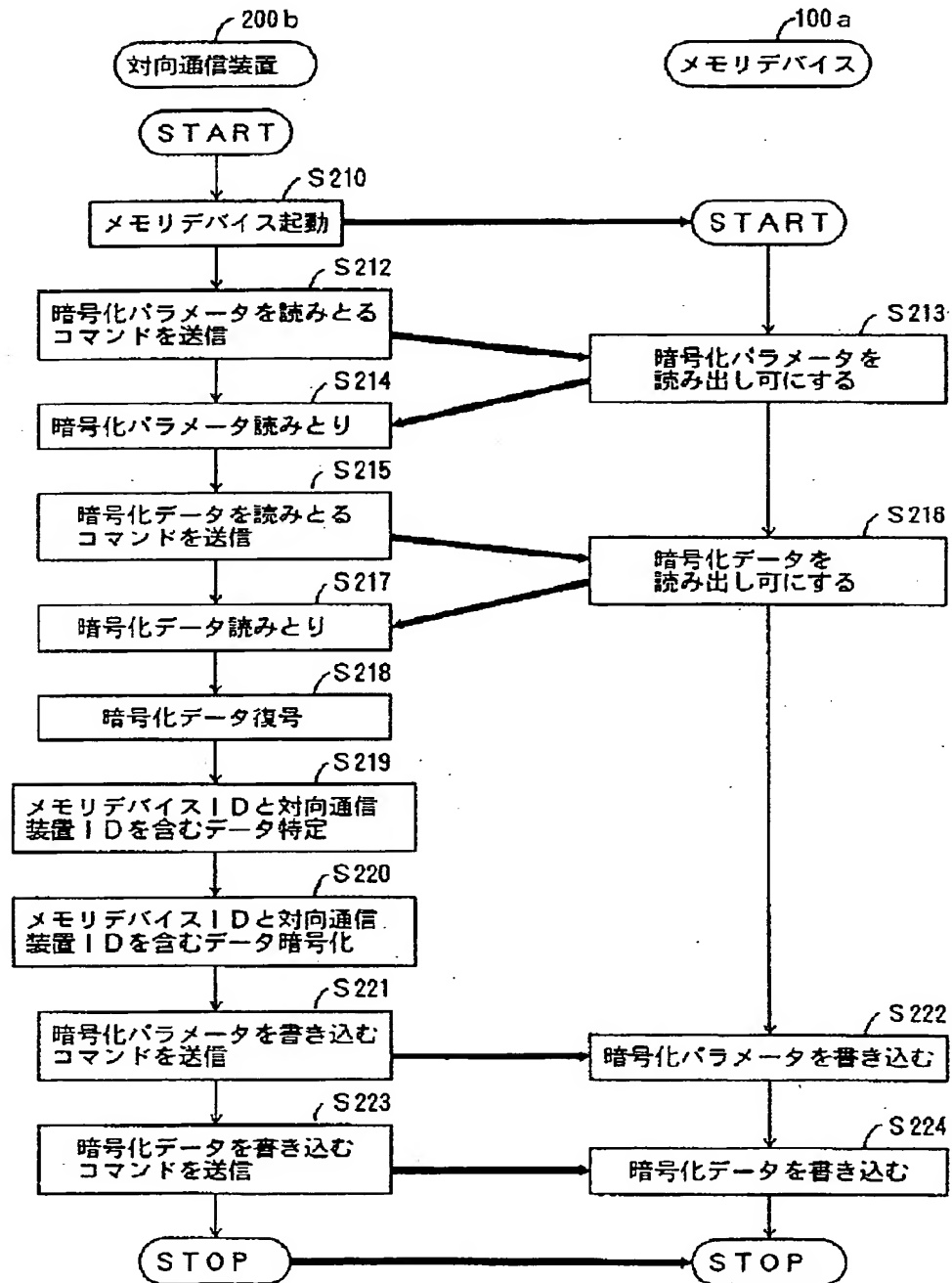
【 図 1 1 】

本発明の第2の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作を示すフローチャート



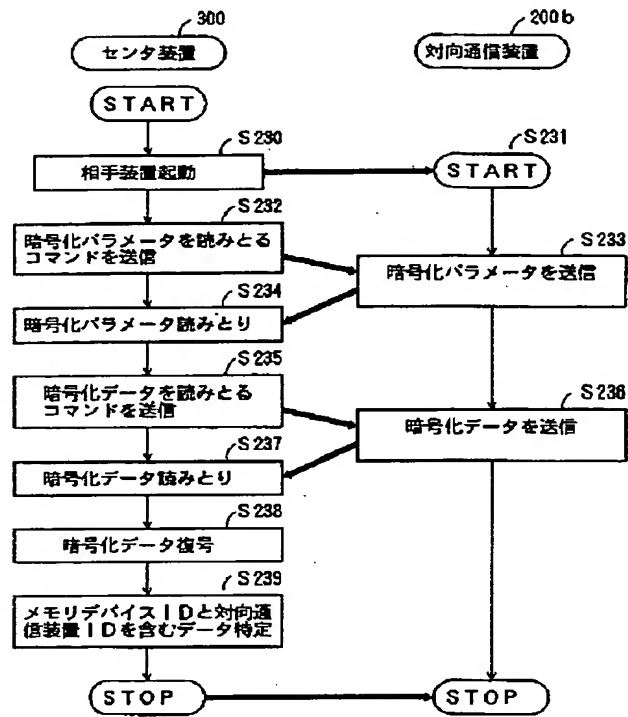
【 図 12 】

本発明の第2の実施例のメモリデバイスと対向通信装置が
2回目以降にやり取りする際の動作のフローチャート



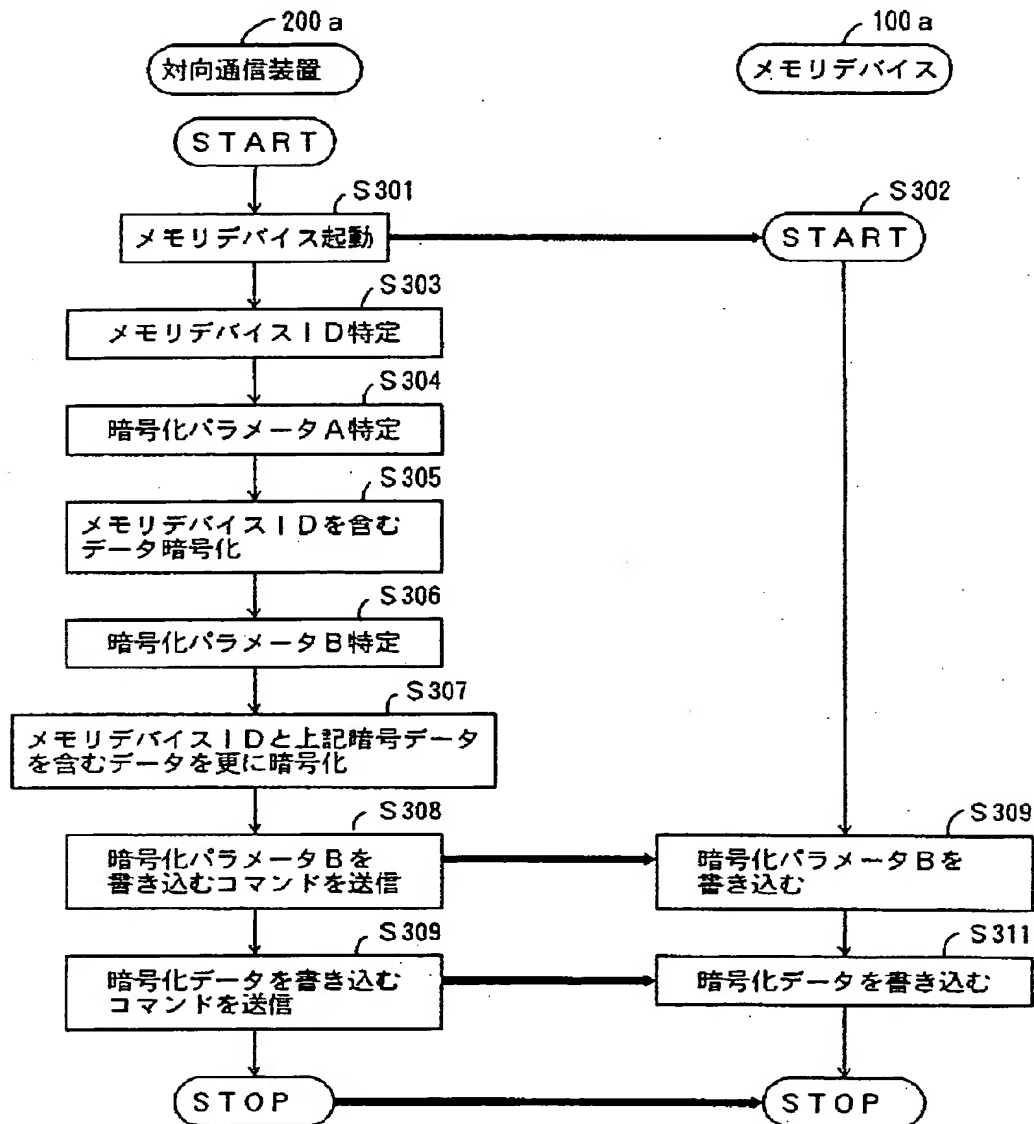
【 図 1 3 】

本発明の第2の実施例の対向通信装置と
センタ装置との動作のフローチャート



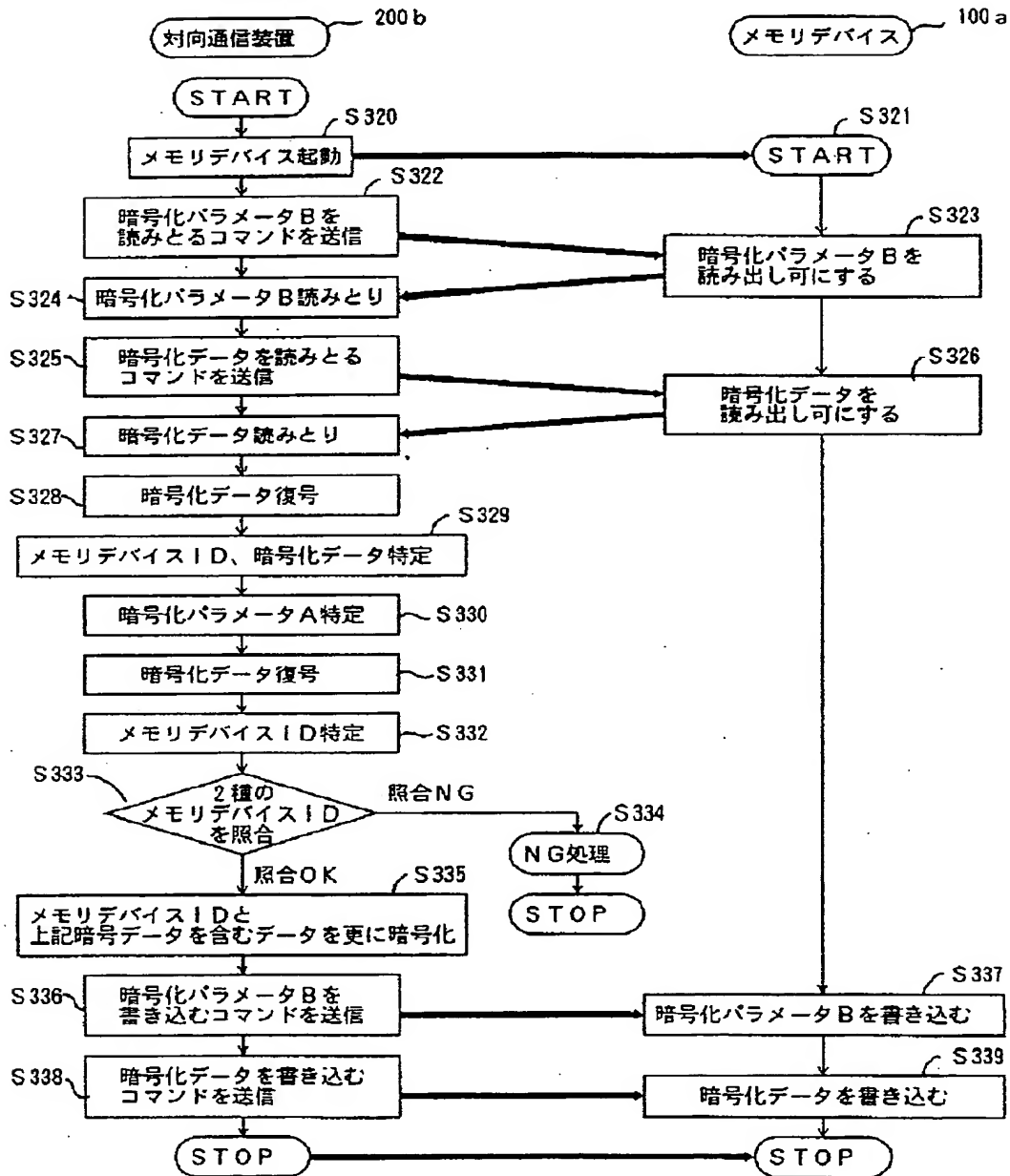
【図15】

本発明の第3の実施例のメモリデバイスと対向通信装置が
最初にデータをやり取りする際の動作のフローチャート



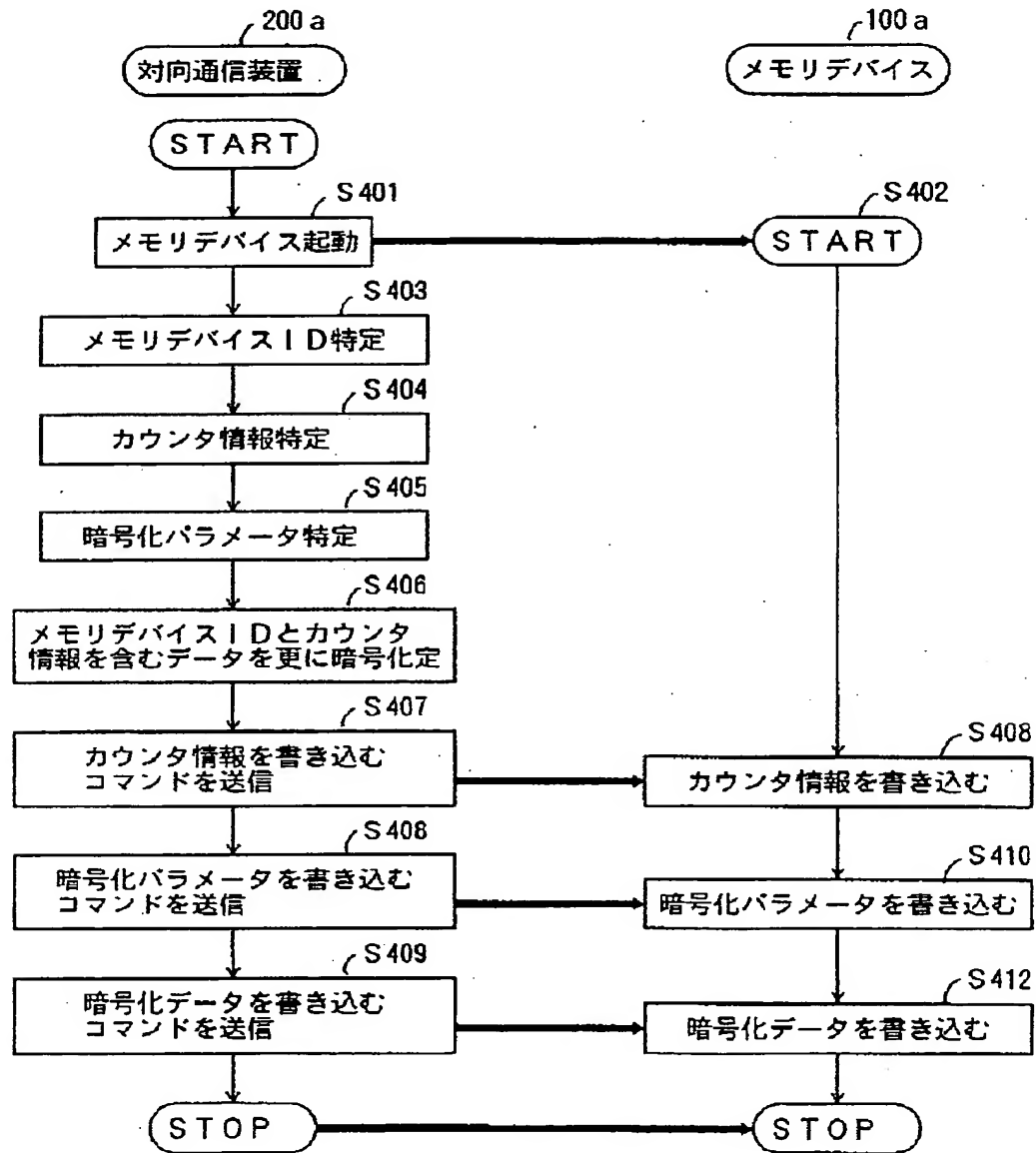
【図 16】

本発明の第3の実施例のメモリデバイスと対向通信装置が
2回目以降にやり取りする際の動作のフローチャート



【図 18】

— 本発明の第4の実施例のメモリデバイスと対向通信装置が
最初にデータをやり取りする際の動作のフローチャート



【 図 1 9 】

本発明の第 4 の実施例のメモリデバイスと対向通信装置が
2 回目以降にやり取りする際の動作のフローチャート

